Ring Homomorphisms and Ideals

Let R, S be rings. A **ring homomorphism** is a map

$$\phi : R \longrightarrow S \qquad \text{s.t. } \forall a, b \in R$$

- $\phi(a+b) = \phi(a) + \phi(b)$ [Abelian group hom.]
- $\phi(ab) = \phi(a)\phi(b)$

If ϕ is 1-1 and onto $\iff$ ϕ is an isomorphism

Def For a ring hom $\phi : R \to S$ define

$$\ker(\phi) = \{ r \in R \mid \phi(r) = 0 \}$$

Ex for any $n \in \mathbb{Z}$ define

$$\phi : \mathbb{Z} \longrightarrow \mathbb{Z}_n$$
$$a \longmapsto a \pmod n$$

$$\phi(a+b) = a+b \bmod n = (a \bmod n) + (b \bmod n) = \phi(a) + \phi(b)$$

$$\phi(ab) = ab \bmod n = (a \bmod n)(b \bmod n) = \phi(a)\,\phi(b)$$

$$\ker(\phi) = n\mathbb{Z}$$

i.e $\phi : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$

i.e $\phi(\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$

$\| $

$\mathbb{Z}_n$

Ex | fix $\alpha \in [a,b] \subseteq \mathbb{R}$

$\phi_\alpha : C[a,b] \longrightarrow \mathbb{R}$

$f \longmapsto f(\alpha)$

$$\phi_\alpha(f+g) = (f+g)(\alpha) = f(\alpha) + g(\alpha) = \phi_\alpha(f) + \phi_\alpha(g)$$

$$\phi_\alpha(fg) = (fg)(\alpha) = f(\alpha)g(\alpha) = \phi_\alpha(f) \cdot \phi_\alpha(g)$$

Prop | Let $\phi : R \to S$ be a ring homomorphism

- If R is commutive then $\phi(R)$ is commutive
- $\phi(0_R) = 0_S$
- Suppose $1_R \in R$, If ϕ is onto then $1_S \in S$ and $\phi(1_R) = 1_S$
- If R is a feild and $\phi(R) \neq \{0\}$ then $\phi(R)$ is a feild

Proof Practice problem

Def: An **ideal** I in a ring R is:

- I is a subring of R
- If $a \in I$, $r \in R$

  $\Rightarrow ar \in I$ and $ra \in I$

  $\Updownarrow$

  that is $rI \subseteq I$ and $Ir \subseteq I$

Ex: $\{0\}$, and R are always ideals of R

$n\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

Remark: Let R to be a ring with $1 \in R$

If I is an ideal and $1 \in I$

$\Rightarrow I = R$ since for $r \in R$ $1 \cdot r = r \in I$

since I is an ideal.

Def: Let R be a commutative ring with $1 \in R$

For any $a \in R$

$$\langle a \rangle = \{ ar \mid r \in R \}$$

↑ The principal ideal of a in R

Check this is an ideal:

$\langle a \rangle$ is a subring

- $\langle a \rangle$ is non-empty since $0 = a0 \in \langle a \rangle$

  $a = a \cdot 1 \in \langle a \rangle$
- $\langle a \rangle$ is closed under addition since $r + r' \in R$

  $ar, ar' \in \langle a \rangle = ar + ar' = a(r+r') \in \langle a \rangle$

L • If $ar \in \langle a \rangle \Rightarrow -ar \in \langle a \rangle$

For any $ar \in \langle a \rangle$, $s \in R$

$$s(ar) = a\overset{n \in R}{sr} \in \langle a \rangle$$

$\therefore$ $\langle a \rangle$ is an ideal of R.

If R commutative ring, $I \subseteq R$, we can also define

$$I = \langle a_1, \ldots, a_n \rangle = \{ h_1 a_1 + \cdots + h_n a_n \mid h_1, \ldots, h_n \in R \}$$

↑ this is also an ideal

• An integral domain where every ideal is principal is called a principal ideal Domain P.I.D

Theorem $\mathbb{Z}$ is a principle ideal domain

Proof: • $\{0\} = \langle 0 \rangle$ is principle

Let I be any non-zero ideal in $\mathbb{Z}$

$\Rightarrow$ There exists some positive $m > 0$ s.t. $m \in I$

$\therefore$ I contains a non-empty subset of $\mathbb{N} = \{1, 2, \ldots\}$

By the well ordering principle $\Rightarrow \exists$ a least positive integer $n \in I$

Choose an arbitray $a \in I$, by the division algorithm

$\exists\ q, r \in \mathbb{Z}$ s.t.

$a = \underbrace{nq}_{\in I \text{ since } n \in I} + r$ where $0 \leq r < n$

$r = \underbrace{a - nq}_{\in I}$

$\therefore\ r \in I$, and $r < n$ and $r \geq 0$

$\Rightarrow r = 0$ since n is the least positive integer in I

$\therefore\ a = nq \quad \forall\ a \in I$

$\therefore\ I = \langle n \rangle$ ∎

Kernels and Quotient Rings

Prop The kernel of any ring homomorphism $\phi : R \to S$ is an ideal in R

[$\ker(\phi)$ is an ideal]

Proof: From groups we know $\ker(\phi)$ is an additive subgroup of R

Let $r \in R$, $a \in \ker(\phi)$. Show $ar \in \ker(\phi)$ and $ra \in \ker(\phi)$

$$\phi(ar) = \phi(a)\phi(r) = 0_S \cdot \phi(r) = 0_S$$

$$\phi(ra) = \phi(r)\phi(a) = \phi(r) \cdot 0_S = 0_S$$

$\therefore\ ra, ar \in \ker\phi$ $\therefore$ $\ker(\phi)$ is an ideal. ∎